(a) Destroy by any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction.

(b) Degauss or overwrite magnetic tapes or other magnetic medium.

(c) Dispose of paper products through the Defense Reutilization and Marketing Office (DRMO) or through activities who manage a base-wide recycling program. The recycling sales contract must contain a clause requiring the contractor to safeguard privacy material until its destruction and to pulp, macerate, shred, or otherwise completely destroy the records. Originators must safeguard Privacy Act material until it is transferred to the recycling contractor. A federal employee or, if authorized, a contractor employee must witness the destruction. This transfer does not require a disclosure accounting.

Subpart H—Privacy Act Exemptions

§806b.27 Requesting an exemption.

A system manager who believes that a system needs an exemption from some or all of the requirements of the Privacy Act should send a request to SAF/AAIA through the MAJCOM or FOA Privacy Act Officer. The request should detail the reasons for the exemption and the section of the Act that allows the exemption. SAF/AAIA gets approval for the request through SAF/AA and the Defense Privacy Office.

§806b.28 Exemption types.

(a) A general exemption frees a system from most parts of the Privacy Act.

(b) A specific exemption frees a system from only a few parts of the Privacy Act.

§806b.29 Authorizing exemptions.

Only SAF/AA can exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions only if SAF/AA previously approved and published an exemption for the system in the FEDERAL REGISTER. Appendix C of this part lists the systems of records that have approved exemptions.

§806b.30 Approved exemptions.

Approved exemptions exist under 5 U.S.C. 552a for:

(a) Certain systems of records used by activities whose principal function is criminal law enforcement (subsection (j)(2)).

(b) Classified information in any system of records (subsection (k)(1)).

(c) Law enforcement records (other than those covered by subsection (j)(2)). The Air Force must allow an individual access to any record that is used to deny rights, privileges or benefits to which he or she would otherwise be entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source) (subsection (k)(2)).

(d) Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection (k)(4)).

(e) Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection (k)(5)).

(f) Qualification tests for appointment or promotion in the federal service if access to this information would compromise the objectivity of the tests (subsection (k)(6)).

(g) Information which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection (k)(7)).

Subpart I—Disclosing Records to Third Parties

§806b.31 Disclosure considerations.

Before releasing personal information to third parties, consider the consequences, check accuracy, and make sure that no law or directive bans disclosure. You can release personal information to third parties when the subject agrees orally or in writing. Air Force members consent to releasing